LOCALIZED NETWORK AUTHENTICATION AND SECURITY USING TAMPER-RESISTANT KEYS

ABSTRACT OF THE DISCLOSURE

[0075] The invention provides a secure Wi-Fi communications method and system. In an embodiment of the invention, unique physical keys, or tokens, are installed at an access point and each client device of the network. Each key comprises a unique serial number and a common network send cryptographic key and a common network receive cryptographic key used only during the authentication phase by all components on the LAN. Each client key further includes a secret cryptographic key unique to each client device. During authentication, two random numbers are generated per communications session and are known by both sides of the wireless channel. Only the random numbers are sent across the wireless channel and in each case these numbers are encrypted. A transposed cryptographic key is derived from the unique secret cryptographic key using the random numbers generated during authentication. Thus, both sides of the wireless channel know the transposed cryptographic key without it ever being transmitted between the two.